REMARKS

Claims 1-35 and 37-41 are pending in the application. Claims 1, 9, 15, 21, 27, and 35 are independent claims. Claim 36 has been cancelled.

Claim 35 has been rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. In response, claim 35 has been amended.

Claims 1-8, 15-17, 21-24, and 27-34 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,177,421 ("Buer"). Claims 9-13 and 35-41 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Buer in view of M.J.B. Robshaw, "On Recent Result for MD2, MD4, and MD5" ("Robshaw"). Claims 18-20, 25, and 26 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Buer in view of U.S. Patent No. 5,365,588 ("Bianco"). Claim 14 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Buer in view of Robshaw and Bianco.

In response, it is argued that each of claims 1-41 include at least one limitation not disclosed by Buer, Robshaw, or Bianco.

For example, independent claim 1 requires a plurality of pipeline stages to perform an inner loop of a hash algorithm, the plurality of pipeline stages comprising at least as many pipeline stages as there are iterations of the inner loop to be performed, wherein each iteration of the inner loop is performed by a dedicated pipeline stage. Buer does not disclose this limitation. Buer describes pipeline control logic that "ensures that the outer hash operation for one data payload is performed in parallel with the inner hash operation of the next data payload" (column 6, lines 25-29). In other words, Buer describes pipelining an iteration of the outer loop with an iteration of the inner loop, such that one iteration of the outer loop is performed in parallel with one iteration of the inner loop. Buer does not describe that one iteration of the inner loop is performed in parallel with another iteration of the inner loop and does not describe that each iteration of the inner loop is performed by a dedicated pipeline stage. In contrast, independent claim 1 requires that each iteration of the inner loop is performed by a dedicated pipeline stage.

The examiner incorrectly argues that Figure 2 of Buer "illustrates several ... hash engines dedicated for parallel inner hash operations." Figure 2 of Buer does not illustrate

several hash engines dedicated for parallel inner hash operations. Figure 2 of Buer illustrates only two hash engines dedicated for inner hash operations, engines 210 and 212. These two hash engines are not dedicated for parallel inner hash operations. Engine 210 is for MD5 hash operations and engine 212 is for SHA1 hash operations. In contrast, the present invention, as set forth in claim 1, requires at least as many pipeline stages as there are iterations of the inner loop to be performed. Figure 2 of Buer shows only one engine for only one iteration of an MD5 hash operation, and only one engine for only one iteration of an SHA1 hash operation. Figure 2 of Buer does not show, and Buer does not describe at least as many pipeline stages as there are iterations of the inner loop to be performed.

Each of the other independent claims of the present application includes an analogous limitation that, based on the above argument, is not disclosed by Buer, Robshaw, or Bianco. Furthermore, each of the dependent claims of the present application includes at least one limitation not disclosed by Buer, Robshaw, or Bianco, based on their dependence on an independent claim including a limitation not disclosed by Buer, Robshaw, or Bianco. Therefore, the rejections of claims 1-35 and 37-41 based on Buer or any combination of Buer with Robshaw and Bianco is improper.

CONCLUSION

Based on the foregoing, it is respectfully submitted that the rejections of claims 1-35 and 37-41 have been overcome, and that claims 1-35 and 37-41 are in condition for allowance. The applicant therefore respectfully requests the issuance of a Notice of Allowance. Please charge any necessary fees, including extension fees, to our Deposit Account No. 50-0221.

Respectfully submitted,

Date: April 7, 2009

/Thomas R. Lane/
Thomas R. Lane
Registration No. 42,781